- 1 1. A method of preventing the repudiation of digitally-signed electronic documents,
- 2 the method comprising the steps of:
- 3 receiving a plurality of electronic documents during a first and second time
- 4 interval;
- forming a message digest for each of the plurality of electronic documents;
- forming a first super-message digest derived at least in part from each of the
- 7 message digests received during the first time interval;
- forming a second super-message digest derived at least in part from each of the
- 9 message digests received during the second time interval and from the first super-
- 10 message digest;
- transmitting the second super-message digest to a timestamp authority and
- 12 receiving a timestamp therefrom; and
- recording each of the message digests, first and second super-message digests,
- 14 and timestamp in an audit log.
- 1 2. The method of claim 1 wherein at least one of the plurality of electronic
- documents corresponds to a file attachment in an electronic mail message.
- 1 3. The method of claim 1 wherein the first and second time intervals are pre-
- 2 determined.

- 1 4. The method of claim 1 wherein the duration of the first and second time intervals
- are dynamically determined from a number of electronic documents anticipated during a
- 3 particular time of day.
- 1 5. The method of claim 1 further comprising the step of recording a timestamp
- 2 associated with the first super-message digest in the audit log.
- 1 6. The method of claim 5 wherein the first super-message digest is further derived
- 2 from the timestamp associated with the first super-message digest and from a prior super-
- 3 message digest.
- The method of claim 5 wherein the second super-message digest is further derived
- 2 from the timestamp associated with the first super-message digest.
- 1 8. A method of securely delivering an electronic document, the method comprising
- 2 the steps of:
- at a message server associated with a sender of the electronic document,
- 4 computing a symmetric key from message parameters associated with the
- 5 electronic document and from a hidden parameter associated with the message server
- 6 using a predefined algorithm;
- 7 encrypting the electronic document using the symmetric key;
- 8 transmitting the encrypted electronic document and the message parameters to at
- 9 least one recipient;

- at a web server coupled to the recipient of the encrypted electronic document,
- receiving identification data associated with the recipient;
- receiving the message parameters transmitted to the recipient;
- comparing the identification data associated with the recipient with the received
- message parameters;
- upon matching the identification data with at least some of the received message
- parameters, dynamically computing the symmetric key from the received message
- parameters and the hidden parameter associated with the message server using the
- predefined algorithm; and
- providing the symmetric key to the recipient.
- 1 9. The method of claim 8 wherein the electronic document is digitally signed.
- 1 10. The method of claim 8 wherein the message parameters include a recipient list
- and a hash of the electronic document.
- 1 11. The method of claim 8 wherein the electronic document and message parameters
- 2 are transmitted to the recipient in an electronic mail message.
- 1 12. The method of claim 11 wherein the received message parameters are posted to
- 2 the web server via an HTML form included in the electronic mail message.

- 1 13. The method of claim 8 wherein the identification data includes a user ID and
- 2 password previously registered by the web server.
- 1 14. The method of claim 8 wherein the message server and the web server are
- 2 controlled by the sender of the electronic document.
- 1 15. A method of securely delivering an electronic document via a web server, the
- 2 method comprising the steps of:
- 3 receiving a symmetrically encrypted electronic document and parameters
- 4 associated therewith, the parameters including a recipient list associated with the
- 5 electronic document;
- receiving identification data from the recipient via a communications network and
- 7 comparing at least some of the received parameters therewith;
- 8 upon matching the identification data and the at least some of the received
- 9 parameters, dynamically computing a symmetric key from the received parameters;
- decrypting the electronic document using the symmetric key; and
- displaying the decrypted document on a web page accessible to the recipient.
- 1 16. The method of claim 15 further comprising the step of transmitting a message to
- a sender of the symmetrically encrypted electronic document after matching the
- 3 identification data and the received parameters.